

NAVAL WAR COLLEGE
Newport, R.I.

CREATING RULES OF ENGAGEMENT FOR INFORMATION WARFARE:
EXAMINING THE POLICY IMPLICATIONS OF INTERNATIONAL LAW

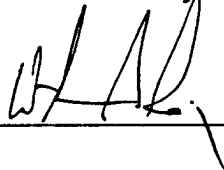
by

William A. Roig

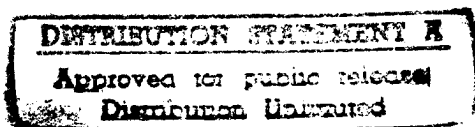
Commander, U.S. Naval Reserve

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: 

13 June 1997



Paper directed by
Captain G. W. Jackson, USN
Chairman, Department of Joint Military Operations

19 May 1997
Commander Raymond H. Carlson, JAGC, USN
Faculty Advisor

19970814 156

DTIC QUALITY INSPECTED 1

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED			
2. Security Classification Authority:			
3. Declassification/Downgrading Schedule:			
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.			
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT			
6. Office Symbol: C		7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207	
8. Title (Include Security Classification): CREATING RULES OF ENGAGEMENT FOR INFORMATION WARFARE: EXAMINING THE POLICY IMPLICATIONS OF INTERNATIONAL LAW (U)			
9. Personal Authors: CDR WILLIAM A. ROIG, USNR			
10. Type of Report: FINAL		11. Date of Report: 13 JUNE 1997	
12. Page Count: 19			
13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.			
14. Ten key words that relate to your paper: INFORMATION WARFARE; ATTACK; USE OF FORCE; PRESENCE; CRISIS PREVENTION; CONFLICT			
15. Abstract: Achieving the full revolutionary impact of information warfare requires distinguishing the methods of information attack from other forms of warfare on policy and legal grounds. Information attack represents a revolutionary new form of warfare from a legal perspective because it allows a severe effect, and therefore intense coercion, to occur with little or no violence and little traditional destruction.			
16. Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users
17. Abstract Security Classification: UNCLASSIFIED			
18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19. Telephone: 841-6461		20. Office Symbol: C	

CREATING RULES OF ENGAGEMENT FOR INFORMATION WARFARE:
EXAMINING THE POLICY IMPLICATIONS OF INTERNATIONAL LAW

ABSTRACT

Achieving the full revolutionary impact of information warfare requires distinguishing the methods of information attack from other forms of warfare on policy and legal grounds. Information attack represents a revolutionary new form of warfare from a legal perspective because it allows a severe effect, and therefore intense coercion, to occur with little or no violence and little traditional destruction. This result is a complete anomaly when compared to traditional warfare which results in more severe effects only through greater destruction and intense violence. Examining the use of force from a policy perspective suggests that the effect of information warfare could have a revolutionary impact on the rules pertaining to the use of force. To gain the full impact from the "revolution in military affairs" represented by information warfare, lawyers and policy makers will have to work together with engineers to create a full continuum of information warfare capabilities which cover the full spectrum of military activity from presence and crisis prevention to full hostilities. Rules of engagement allowing the full participation of information warfare at each stage of conflict will be needed to fully effectuate the policy behind international law's attempt to regulate the use of force toward preferred policy goals. This paper suggests how such rules of engagement might be constructed and calls for focused research on a set of questions to allow the rules to effectuate the policy behind international law.

I. Introduction

Technological innovations developing as information warfare are spurring tactical and doctrinal developments that will have a dramatic impact at the operational level of war. True revolutions in military affairs (RMAs) however, are developed on three interdependent axes: 1) technological development (new things); spurs 2) doctrinal development; and 3) organizational changes to take full advantage of the new capabilities. Only when all three sets of innovations are put in place is the full advantage of revolutionary technological change realized. New hardware alone does not make a revolution in military affairs.

Many legal observers are assuming that no matter how innovative the new technologies prove, the changes to warfare wrought by information warfare will be governed by evolving the existing rules of international law and that there will be no "revolution in legal affairs."¹ The conservative application of existing rules can be used as an approach to bring order to information warfare concepts and capabilities. But no one is asking the question as to whether it would be advantageous to drive the development of international law along new lines based on the unprecedented nature of information warfare.

This paper argues that only by demonstrating the inapplicability of existing international law to information warfare can the full revolutionary potential of this new type of warfare be realized. A shift in the legal paradigm governing the international security order could occur by examining the preferred policy options of that order and using the revolutionary techniques of information warfare to effectuate them. The question becomes one of what rules

should be adopted to effectuate a set of preferred policy options. Only by avoiding a mechanistic application of the existing rules will the full potential of information warfare be reached. Lawyers will have to play a constructive, developmental role to create the RMA because of the way information warfare can redefine the use of force. Looking at the policy behind the U.N. Charter and the Law of Armed Conflict it is possible to examine how new rules might take shape.

II. The Unique Capabilities of Information Warfare

If information warfare represents nothing new then there will be no need for developing specific international law to govern it. If on the other hand, information warfare is revolutionary and does present the commander with new types of capabilities, there may be the need for such development. How can we know?

Information warfare was recently sub-divided in two important ways. The new term "information operations" reflects the realization that much of what was previously known as information "warfare" would actually occur in peacetime or in the pre-hostilities phase of a conflict. Information operations include the transition to information warfare.

Information warfare has also been sub-divided into information based warfare and information attack. The revolution in information based warfare is largely the result of the enormous storage and processing capabilities of modern high speed computers multiplied many times over through the fusion of data made possible by high speed transfer rates on interconnected computer networks and the spread of processing capability throughout the armed forces.

Information based warfare makes more information available to the warrior for

force employment. Precision guided munitions are an example of information based warfare. The traditional methods of command and control warfare fit easily into information based warfare: deception, electronic warfare (the exception which overlaps with information attack), physical destruction, psychological operations, and operational security.

Information attack, the other main branch of information warfare, targets the operation of an opponent's information systems with intrusion or directed energy to attack the functioning of that system. When placed on a continuum of relative intrusiveness, a typology of information attack capabilities is suggested:

Processes and data can be slowed down.

Processes and data can be isolated.

Processes can be interrupted.

Processes can be deceived.

Processes and data can be altered.

Processes can be shut down.

Processes and data can be corrupted.

Processes and data and equipment can be destroyed.

Collateral damage can occur.

Creating a continuum of information attack capabilities is necessary to allow information attack to be used over the entire spectrum of warfare and the entire crisis cycle from presence to crisis management to hostilities. Building capabilities which stretch over the spectrum will be vital to give the commander a full range of escalatory and de-escalatory information warfare tools appropriate to the phase of the operation.

Examining the nature of information attack and comparing it with existing forms of warfare reveals its unique character. While information warfare

promises to have tremendous effects on the functioning of a military, economy, or government, it at the same time promises little physical destruction and very little or no violence. Rather than destroying the physical infrastructure or people of a state or military force, their systems (equipment and infrastructure) just cease to function or do not function correctly. If these systems cease to function in a truly non-destructive manner such that their paralysis could be reversed by computer code, the result is a complete anomaly in the history of warfare -- intense "destruction" (or severe effects) of systems and therefore intense coercive effect without violence. The result is even more revolutionary if the destructive processes are reversible by reprogramming.

III. International Law Applicable to Information Warfare

A. Rules as Statements of Policy Values

There are several ways to conceptualize what constitutes international law. International law is a body of rules which purport to bind states to acting according to the norms of accepted international behavior. These rules as norms are found in the various sources of international law. International law can also be examined from a policy perspective.³ Rules are not made in a vacuum -- they are made to translate policies preferred by the international community into an international order. The international order is often criticized as being a loose order characterized by anarchy as there is no centrally recognized authority to enforce international law.⁴ Enforcement operates in a permissive regime where the actors in the international order are left to abide by the rules of that order through comity and reciprocity and to enforce the law on the recalcitrant

through self-help. This order is enshrined in the United Nations Charter and represents the backdrop of the international security order.

Three trends are noticeable in the development of this security order. First, a ring is slowly tightening on the permissible uses of force. Second, in the narrowly circumscribed area of permissible uses for force, the type of force that is permissible is narrowing. And third, force, when used, is increasingly used collectively to uphold and police the international order. Behind each of these trends is a set of policy values or choices states are making about what sort of international order they find desirable.

If we are earnest about using information warfare to its fullest possibilities then we must construct its capabilities across the full spectrum of conflict with a full range of response capabilities to get out in front of the three trends mentioned above. It should be demonstrated that information warfare, as a technique of applying coercion or force, is a value maximizing means of enforcing the international security order. To find out how information warfare can be used to maximize the policy values of the international security order embodied in international law we must examine the rules and policy goals of that order.

B. The Prohibition on the Use of Force

The aggressive use of force as an instrument of national policy is effectively prohibited by Article 2(4) of the Charter of the United Nations in language which proscribes "the threat or use of force against the territorial integrity or political independence of any state."⁵ Elective war for political change or to maximize national self-interest is prohibited.⁶ This prohibition grew out of the intensely destructive experience of World War I and was first

embodied in the Kellogg-Briand Pact of 1928.⁷ The resort of going to war had become so destructive as to take away any advantage it might hold as a policy instrument.

Article 51 of the Charter reserves to states the inherent right of self-defense.⁸ Since there is no higher sovereign than the sovereign authority of states to enforce international order, Article 51 operates as the enforcement mechanism for Article 2(4). While states are prohibited from using force as a preferred agent of change in international relations they retain an inherent right to use force to deter or correct an illegal use of force.

This brings us directly to the question of whether information warfare constitutes the use of force under the U.N. Charter. If information attack capabilities are placed on the spectrum of conflict, are there capabilities that can be used coercively in the pre-hostilities phase without constituting a use of force and therefore the commencement of hostilities?⁹ What distinguishes information warfare from all previous forms of warfare is that while it promises great destruction of modern systems and infrastructure and hence a highly coercive potential, it accomplishes both without traditional violence. This result is at odds with the original policy behind the Charter's prohibition on force, that modern warfare and the concomitant loss of life were increasingly making warfare too destructive and too violent to legitimate. If the policy goal behind Article 2(4) is to minimize the destructive effects of war then certain techniques of information attack might become the self-defense weapons of choice to be encouraged because of their lack of violence and potential for inducing paralysis without traditional destruction. In this manner information warfare could have far reaching effects on international law and the use of force.

C. Regulation of the Use of Force

The Law of Armed Conflict¹⁰ assumes that states engaged in hostilities nonetheless have incentives to regulate their use of force. Traditional law breaks these concerns down into several categories the most significant of which for our purposes are necessity and proportionality.

1. Necessity

The rule of necessity operates to allow only those actions which are imperative for defeating the enemy and "forbids acts which go beyond this and cause injury to persons or damage to property not essential to achieving this end."¹¹ Necessity acts to limit the amount of force to that which is rationally connected to the allowed purpose and becomes a rule of reasonableness in a particular context.¹² Necessity effects both the means employed as instruments of force and the objects against which that force is directed.¹³

The policy behind the rule of necessity limits the amount of death and destruction allowed. Senseless destruction, killing, or maiming, which serves no military purpose toward defeating the enemy, is prohibited. In practice the rule allows the employment of a wide variety of weapons not otherwise prohibited against the enemy's military forces. When force is directed against the enemy's war making potential in the civilian economy however, the application of the rule becomes more strict requiring demonstration that the target affects the ability or will of the enemy to fight.¹⁴ However, in attacking the information infrastructure of a state with information attack, violence and hence killing and maiming of civilians is minimized in a revolutionary manner. Compare this sort of attack to paralyze the war making potential of an economy with a conventional bombing attack to accomplish the same result. Of course information attack could

still cause some collateral damage -- hospitals shut down, electricity shut off, deliveries of essential goods interrupted.

2. Proportionality

The rule of proportionality acts to limit the amount of force used in self-defense to a reasonable amount of force as compared to the amount of unlawful force used by the initiator. The policy of the rule acts to limit the amount of violence and destruction authorized under the self-defense concept. For instance, every unlawful use of force does not justify total war.

In practice, the application of the proportionality rule causes some of the most novel problems concerning the use of information warfare within the constraints of international law. Proportionality presents novel concerns to information warfare because of its great destructiveness to systems with minimal violence and because of its great potential for asymmetric use.

Great "destructiveness" without violence and minimized physical destruction is something new that information attack brings to warfare. It was not foreseeable when the U.N. Charter was written. Consider the scenario where in response to unlawful aggression, a Charter member acts in self-defense with an information attack that shuts down the opposing military. No one is killed, and the "hardware" infrastructure of the military remains intact, but nothing works well enough to conduct credible military operations. All the computers are dead in the military structure. This action in self-defense most likely meets the tests of necessity and proportionality -- probably a type of self-defense act that should be encouraged because of its lack of loss of life and limited physical destruction. Only the memory of the computers was destroyed or perhaps even the computers themselves.

In a second case, an information attack shuts down all the computers, but this time in the civilian sector as well as in the military. The power grid, banking system, and all manner of business communications linked to the national telecommunications system are destroyed or rendered inoperable. No one is killed outright in the attack, but the lack of electrical power might bring increased deaths from other factors -- hospital systems lose power, water pumps stop, traffic lights go out, and so on. Casualties are a consequence of the information attack, but they are not brought on by the violence of the attack. If measured in terms of the total impact on the society, it may be that the attack was extreme, taking away the economy and many forms of social intercourse in one attack. If measured in terms of casualties, or destruction to the physical plant, the hardware of the society, the attack may be viewed as not very destructive and therefore in keeping with the policy behind proportionality -- to limit violence and destruction.

Asymmetric uses of force complicate matters further. Not all states will possess the means of information warfare, nor will all states possess the computer-linked infrastructure that provides worthwhile targets for information attack. A state confronted with an information attack which does not possess the means for information warfare will have to respond with conventional violence if it chooses to use force in self-defense. Similarly, a state may sustain an information attack from another state which is not technologically advanced enough to possess the computer-linked target infrastructure which makes information attack possible. In both of these cases proportionality will be a potential problem. In the case of the state which simply has no information attack capability, the principle of necessity will most likely justify the resort to conventional violent self-defense. That state has no other choice, the best case of necessity.

A technologically advanced state may suffer an information attack from a non-technologically advanced state which nonetheless has acquired information attack capability. Now the advanced, more powerful state will be tempted to resort to conventional violence as a use of force in self-defense. This use seems more disproportional since the more powerful state instead of responding in kind with information attack which minimizes violence, escalates the violence in self-defense.

Another anomaly is that technologically underdeveloped states may find it easy and inexpensive to acquire the technology for information attack. Computer technology is becoming ever cheaper while the target environment is becoming richer as more interdependent computer networks link the economies of the advanced states. Systems linking all states in larger, more universal sets of interdependencies will eventually provide a stabilizing influence when everyone has more to lose. Everyone that is except terrorists and a few rogue states which will be dealt with as criminals in another legal regime outside the scope of this paper.

IV. Divining Rules of Engagement for Information Warfare

A. What are Rules of Engagement?

Rules of Engagement (ROE) are directives from command authorities authorizing the use of force as specified within the rules. By authorizing the use of force under specific circumstances, ROE at the same time limit the use of force -- what is not authorized is prohibited. Force can be limited in a number of ways: 1) the situation where it may be used; 2) the type of force that may be used; 3) on whose authority force may be used; and 4) against whom force may be directed.

With ROE command authorities are able to control the level of hostilities to link the use of force to policy goals, to control more positively certain types of highly destructive fires, and limit destruction to specific military objectives.

B. Developing ROE for Information Warfare

Information warfare techniques need to be factored over the entire continuum of conflict from prevention through crisis management to hostilities. Appropriate technical capabilities need to be designed and fielded appropriate to each stage in the continuum. A potential conflict is evident from the start between the proponents of a quick, decisive knock-out blow and those who will want to use a scaled approach to tighten the screws through coercive diplomacy. Information warfare's promise of severe effects (as opposed to traditional destruction) and high coercion with little or no violence makes its techniques ideally suited to pre-hostilities and conflict management stages.

The separation of peacetime information operations from hostilities needs clear delineation. Rules that are too conservative may leave much of information warfare on the table unused. Rules that are too liberal may push the other side to preemptive attack rather than waiting for the disabling of sophisticated systems by information attack.

C. Four Sets of Rules

Four distinct situations exist inviting the creation of four sets of information warfare ROE each with distinct concerns:

1. Peacetime ROE would govern day-to-day information operations allowing self-defense postures while protecting the security of classified capabilities.

2. Exercise ROE would allow for practice of techniques and the selective showcasing of capabilities for deterrent effect. If all the information attack programs are kept "black" for wartime use the deterrent value of information warfare becomes too speculative to be credible.

3. Demonstration ROE would allow for information warfare "presence" to be felt in a particular area of crisis or potential crisis to allow maximum scaled impact in the prevention and crisis management stages of a conflict. Emphasis would be on measured, controlled responses to exert maximum influence through the techniques of coercive diplomacy.

4. Wartime ROE would allow progressive takedown of enemy systems at the commander's discretion up to the maximum degree allowable under the Law of Armed Conflict in accordance with operational plans.

V. Conclusion: Proposals for Further Development

To get the full measure of capability from information warfare it may be necessary to work backwards from the key innovations and differences that this new form of warfare offers to what type of legal regime would maximize this potential. The practicality and possibility of steering international law in new directions based on the maximization of policy values can then be assessed. As a proposal for continuing research, answering the following questions leads towards a fully effective use of information warfare:

1. What is the policy behind the Law of Armed Conflict?
2. What is the policy behind the prohibition on the use of force?
3. What is the policy behind the inherent right of self-defense?
4. How are these three sets of policy concerns best effectuated by IW?

5. How is information warfare distinguished from conventional warfare?
6. When is information warfare the use of force as defined by Article 2(4)?
7. Is information attack an armed attack?
8. Where is the line between information warfare and information operations?
9. Can information warfare be applied over the entire spectrum of conflict?
10. Will information warfare be useful over the entire spectrum of conflict?
11. Can information warfare be used preemptively?
12. What rules would maximize the revolutionary potential of IW?
13. What rules add to international system stability?
14. What rules maximize the deterrent value of information warfare?
15. What rules maximize the coerciveness of information operations short of war?

Meaningful research will address all these questions serially to allow a cumulative effect of interpreting and applying policy choices. The urgent question becomes "Should the law governing information warfare be left to slow evolution or should we seize the opportunity to distinguish information warfare as something new that will require new law -- something revolutionary?" To make full use of the unique capabilities of information operations, information warfare capabilities need to be developed as something new to be distinguished from more traditional forms of warfare. Understanding the policy concerns behind relevant international law points the way. Military attorneys need to lead the charge to distinguish the technical capabilities, policy, and operational concerns of information warfare in order to secure its full potential. An RMA in this field cannot be secured by engineers alone. Assuming that traditional law is up to the task of maximizing the potential of information warfare amounts to sticking our collective national head in the sand. As the world technological leader, the United States should push for extensive new development in

international law given the unprecedented distinguishing characteristics of information warfare.

NOTES

1. Colonel Phillip A. Johnson, "Notes on Law and Information Warfare" Unpublished Conference Paper, International and Operations Law Division, Headquarters United States Air Force, Washington, D.C.: 13 October 1995.
2. The Charter of the United Nations, Article 2, paragraph 4.
3. Oscar Schachter, International Law in Theory and Practice (London: Martinus Nijhoff Publishers, 1991), 21-27.
4. *Id.*, 9-10.
5. The Charter of the United Nations, Article 2, paragraph 4.
6. John Norton Moore, "Development of the International Law of Conflict Management," in John Norton Moore, Frederick S. Tipson, and Robert F. Turner, National Security Law (Durham, North Carolina: Carolina Academic Press, 1990), 68.
7. *Id.*, 68.
8. The Charter of the United Nations, Article 51.
9. See generally, James N. Bond, "Peacetime Foreign Data Manipulation As One Aspect of Offensive Information Warfare: Questions of Legality under the United Nations Charter Article 2(4)," Unpublished Research Paper, U.S. Naval War College, Newport, RI: 14 June 1996.
10. The Law of Armed Conflict consists of an amalgam of law from various sources (convention, custom, etc.) which applies to the conduct of armed conflict.
11. L.C. Green, The Contemporary Law of Armed Conflict (Manchester: Manchester University Press 1993), 118.
12. Myres S. McDougal and Florentino P. Feliciano, The International Law of War, Transnational Coercion and World Public Order (New Haven: New Haven Press 1994), 218.
13. Green, *op. cit.*, 118.
14. *Id.*, 120-121.

BIBLIOGRAPHY

- Aldrich, Richard W. The International Legal Implications of Information Warfare, INSS Occasional Paper 9, Information Warfare Series, U.S. Air Force Academy, Colorado: USAF Institute for National Security Studies, April 1996.
- Bond, James N. "Peacetime Foreign Data Manipulation As One Aspect of Offensive Information Warfare: Questions of Legality under the United Nations Charter Article 2(4)," Unpublished Research Paper, U.S. Naval War College, Newport, RI: 14 June 1996.
- Brownlie, Ian International Law and the Use of Force By States, Oxford: Clarendon Press; New York: Oxford Univ. Press, 1981.
- _____. State Responsibility. Part I. System of the Law of Nations (Series), Oxford: Clarendon Press, 1983.
- Damrosch, Lori Fisler, Gennady M. Danilenko, and Rein Mullerson Beyond Confrontation. International Law for the Post-Cold War Era, Boulder: Westview Press, 1995.
- _____. and David J. Scheffer, eds. Law and Force in the New International Order, Boulder: Westview Press: 1991.
- George, Alexander L. Forceful Persuasion. Coercive Diplomacy as an Alternative to War, Washington, D.C.: U.S. Institute of Peace Press, 1991.
- Green, L.C. The Contemporary Law of Armed Conflict, Manchester: Manchester University Press, 1993.
- Harley, Jeffrey A. The Role of Information Warfare: Truths and Myths, Unpublished Research Paper, U.S. Naval War College, Newport, RI: 18 March 1996.
- Howard, Michael, George J. Andreopoulos, and Mark R. Shulman, eds. The Laws of War: Constraints on Warfare in the Western World, New Haven: Yale University Press, 1994.
- Howard, Michael, ed. Restraints on War. Studies in the Limitation of Armed Conflict, Oxford, Oxford University Press, 1979.
- Kuschnier, Karl W. "Legal and Practical Constraints on Information Warfare," Unpublished Research Paper, U.S. Naval War College, Newport, RI: 14 June 1996.
- Libicki, Martin "The Emerging Primacy of Information," Orbis, Vol. 40, No.2 Spring 1996, p. 261.
- Libicki, Martin C. What Is Information Warfare?, Fort McNair: National Defense University, Center for Advanced Concepts and Technology, 1996.

- McCoubrey, Hilaire and Nigel D. White International Law and Armed Conflict, Aldershot: Dartmouth Publishing Company, 1992.
- McDougal, Myres S., and Florentino P. Feliciano The International Law of War, Transnational Coercion and World Public Order, New Haven: New Haven Press, 1994., pp. 198-202.
- Moore, John Norton "Low-Intensity Conflict and the International Legal System" in Coll, Ord, and Rose, Legal and Moral Constraints on Low-Intensity Conflict, Newport, R.I.: U.S. Naval War College, International Law Studies, Vol. 67., 1995.
- Moore, John Norton "Development of the International Law of Conflict Management," in John Norton Moore, Frederick S. Tipson, and Robert F. Turner, National Security Law, Durham, North Carolina: Carolina Academic Press, 1990, p. 68.
- Schachter, Oscar International Law in Theory and Practice, London: Martinus Nijhoff Publishers, 1991.
- Schneider, Barry R. and Lawrence E. Grinter, eds. Battlefield of the Future, 21st Century Warfare Issues, Air War College, Studies in National Security No. 3, Maxwell AFB: Air University Press, September 1995.
- Wriston, Walter B. The Twilight of Sovereignty, New York: Charles Scribner's Sons, 1992.
- Zengel, Patricia "Responding With Force To Information Warfare: Legal Perspectives," Unpublished Research Paper, U.S. Naval War College, Newport, RI: March 1997.